Yellow to Turquoise Integration (YeTI) Project

Brett Kettering,
Benjamin McClelland, HPC-5;
Kyle Lamb, HPC-3;
Alex Malin, HPC-DO

Security and access control considerations have prompted LANL to have two completely separate, but essentially mirrored, unclassified high-performance computing (HPC) networks. These networks, called Yellow and Turquoise, share many common but separate components and infrastructure design, as well as the personnel who maintain and upgrade them. Due to inefficiencies and duplicated costs, the Yellow-to-Turquoise Integration (YeTI) project was created to investigate the merging of these network and HPC resources while addressing the security and access controls that prompted the separate networks in the first place. The YeTI project exceeded its initial investigation goal and has implemented the YeTI model on three production HPC machines and has plans for converting all remaining machines in FY13.

Sharing expensive resources and combining the Yellow and Turquoise networks is expected to save LANL millions of dollars in personnel and hardware costs while maintaining demanding standards for the protection and separation of data.

The implementation chosen for YeTI allows the most expensive infrastructure, such as the HPC compute resource, network switches, parallel and network file system space, and archive space, to be shared. System front-ends are not shared, so that we can identify the user's protection level and limit the user's access to those data.

Users may only access data for which they have been authorized and have the appropriate need to know. Turquoise users only see the Turquoise level of data and cannot access Yellow data. New levels of data protection, such as a section for individuals collaborating with a private company, can be added with much less effort than fielding a new system.

HPC resources are configured on a per job basis to allow for computing with data appropriate for the user who is launching the job without hardware partitions or enclaves. There is minimal impact on the user experience on YeTI machines. In some cases, especially where a user operates in both the Yellow and Turquoise environments, the user experience is improved.

Yellow users can still copy and move files between the Turquoise and the Yellow and can use their existing test and development frameworks. Cluster-to-desktop visualization capabilities are still functional and access to the Reconfigurable Advanced Visualization Environment (RAVE) is maintained. There are no changes from the user point of view for managing user and group permissions or other data protection mechanisms.

Originally, users on the Yellow network could only access Turquoise-network systems by going through gateway nodes. Binaries had to be built on special Yellow network compile nodes and then pushed through the gateway nodes to the Turquoise network systems. Direct checkout/checkin and automated development processes was not possible with this setup.

With the new YeTI model, we have provided a system front-end in the Yellow network address space that is connected through a carefully controlled and protected link to the system's private out-of-band network. The existence of the front-end in the Yellow network address space gives Yellow-network-based users access to normal Yellow network resources (e.g., TeamForge, other source code repositories, Mercury, etc.) and allows most development, debugging, testing, etc., processes to occur as they do on systems currently fully based in the Yellow network. The private network link gives the Yellow-network-based users access to the Turquoise-network-based resources of the system (e.g., compute nodes, parallel file systems, etc.). Turquoise network users see no difference in how the system is currently accessed and used.

Future work for the YeTI project includes investigating methods for reducing dependence on user settings for file access control and removing the impacts associated with potential privilege escalations.

The YeTI project has increased the likelihood of unclassified collaborations with other agencies, universities, and laboratories while increasing the security of our open network operations. These security measures are accomplished with no significant development of local software or large purchases.

For more information contact Ben McClelland at ben@lanl.gov.

Funding Acknowledgments
DOE, NNSA, Advanced Simulation and Computing Program; LANL Institutional Computing Program

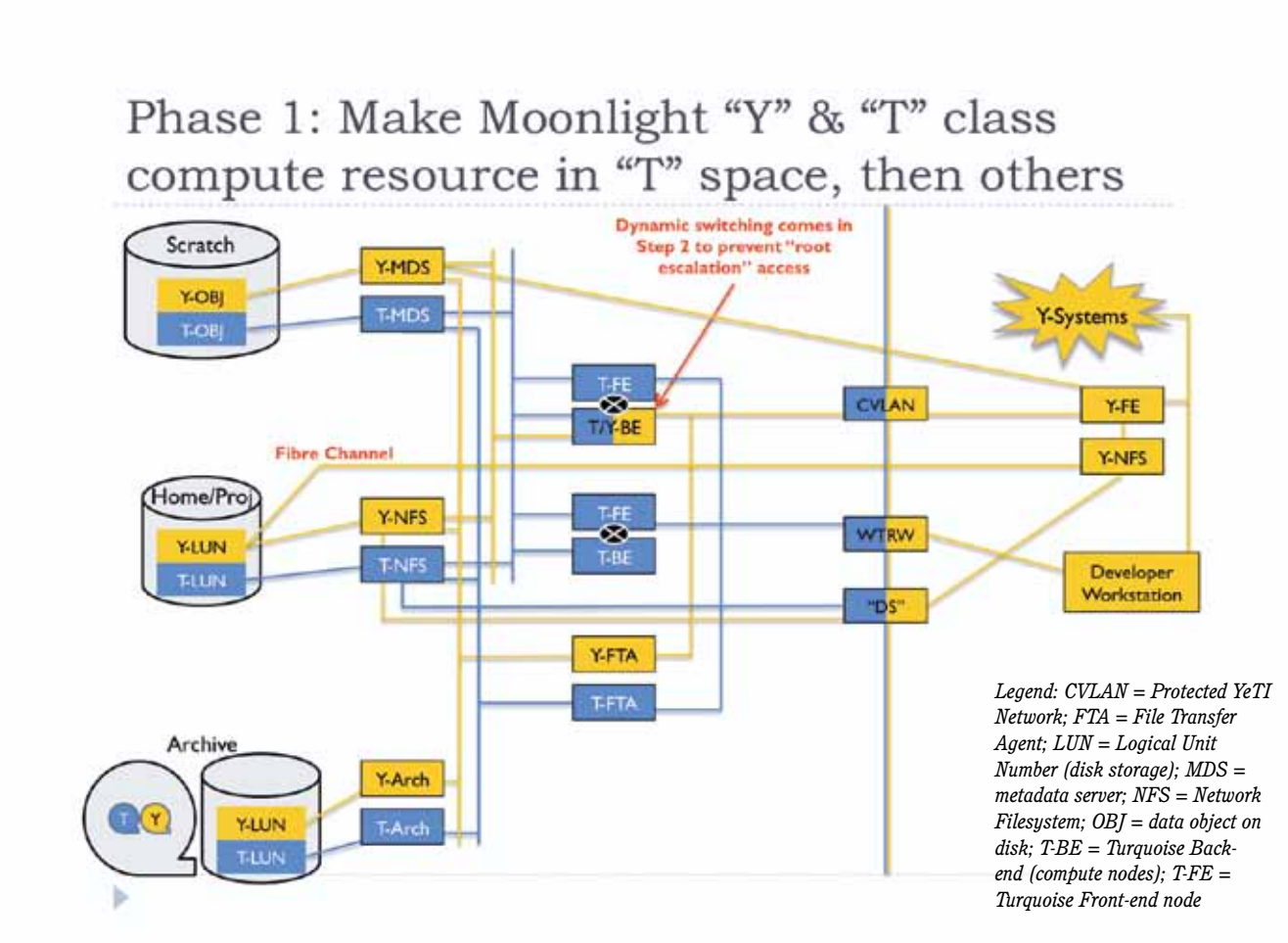

Fig.1. Diagram of the network and cluster modifications for the projects.